

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-132020

(43)Date of publication of application : 09.05.2003

(51)Int.Cl.

G06F 15/00

G06F 13/00

H04L 9/32

(21)Application number : 2001-329307

(71)Applicant : CYBER SIGN JAPAN INC

(22)Date of filing : 26.10.2001

(72)Inventor : KANEKO HISAHIRO

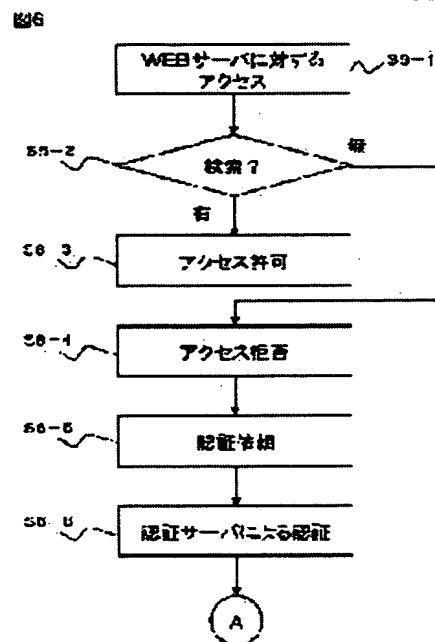
(54) ACCESS CONTROL APPARATUS, AUTHENTICATION APPARATUS AND APPARATUS RELATED TO THEM

NCS-0023

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an apparatus and a program, capable of dynamically changing access control rule.

SOLUTION: When an external terminal 20 accessing to an WEB server 16, if access has not been permitted and the access is refused, the external terminal 20 transmits an authentication request to an authentication server 18, to obtain permission. The authentication server 18 authenticates, based on the signature data included in the authentication request, if the external terminal 20 is an authorized one, and requests to a firewall to set the access control rule to permit 'access controls to be executed', included in the authentication request. The firewall 10 sets the access control rule, based on the request. Accordingly, the access control rule corresponded to a current user can be set, so that a network can be used smoothly.



LEGAL STATUS

[Date of request for examination]

21.10.2004

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-132020

(P 2 0 0 3 - 1 3 2 0 2 0 A)

(43) 公開日 平成15年5月9日 (2003.5.9)

(51) Int. Cl. ⁷	識別記号	F I	テーマコード (参考)		
G06F 15/00	330	G06F 15/00	330	A	5B085
			330	F	5B089
13/00	351	13/00	351	Z	5J104
H04L 9/32		H04L 9/00	673	D	

審査請求 未請求 請求項の数 7 O L (全10頁)

(21) 出願番号 特願2001-329307 (P 2001-329307)

(22) 出願日 平成13年10月26日 (2001.10.26)

(71) 出願人 500120668

日本サイバーサイン株式会社

東京都世田谷区用賀4丁目5番16号 T E
ビル5 F

(72) 発明者 金子 尚浩

東京都世田谷区用賀4丁目5番16号 T E
ビル5 F 日本サイバーサイン株式会社内

(74) 代理人 100109014

弁理士 伊藤 充

F ターム (参考) 5B085 AE25 BA07 BG02 BG03 BG07

5B089 GA11 GA21 GB02 HA10 JB22

KA17

5J104 AA07 KA01 KA16 NA05 PA07

(54) 【発明の名称】 アクセス制御装置及び認証装置及びそれらに関連する装置

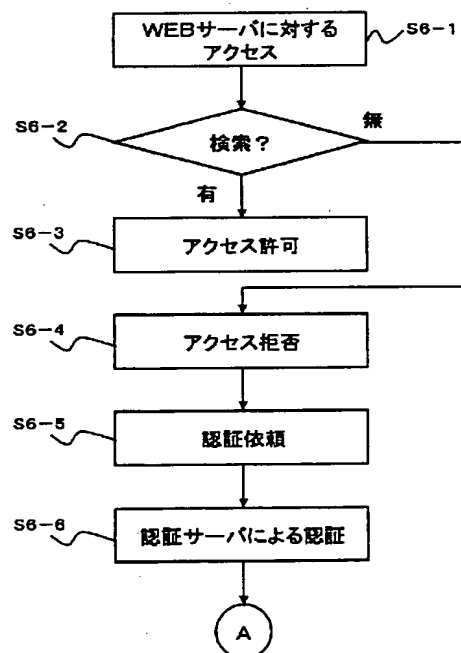
(57) 【要約】

【課題】 アクセス制御ルールを動的に変更しうる装置やプログラムを提供することである。

【解決手段】 外部端末20がWEBサーバ16に対してアクセスを行おうとする。このアクセスが許可されていない場合は、アクセス拒否された場合、外部端末20は、許可を得るために認証サーバ18に認証依頼を送信する。認証サーバ18は、認証依頼中の署名データに基づき認証し、正当な者であれば、認証依頼中に含まれていた「実行したいアクセス内容」を許可するアクセス制御ルールを、ファイアウォール10に設定するように依頼する。この依頼に基づき、ファイアウォール10がアクセス制御ルールを設定する。この結果、現在の使用に対応したアクセス制御ルールが設定できるので、円滑なネットワークの利用が可能である。

NCS-0023

図6



【特許請求の範囲】

【請求項 1】 第 1 ネットワークと、第 2 ネットワーク間のアクセスを制御するアクセス制御装置において、アクセス制御ルールが格納されたアクセス制御テーブルと、

前記第 1 ネットワークから第 2 ネットワークへのアクセス要求があった場合に、要求されたアクセスを、前記アクセス制御テーブルから検索する検索手段と、

前記検索手段が前記アクセスを前記アクセス制御テーブルから見いだせなかった場合に、前記発信元にアクセス拒否を送信する拒否手段と、

前記検索手段が前記発信元を前記アクセス制御テーブルから見いだせた場合に、前記アクセス制御テーブルに格納されたアクセス制御ルールに基づき、アクセスを実行させるアクセス制御手段と、

バイオメトリクス認証結果を第 3 者に渡す認証サーバから、アクセス制御ルールの設定依頼が送信されてきた場合に、前記アクセス制御テーブルの内容を変更、追加又は削除するアクセス制御ルール管理手段と、

を含むことを特徴とするアクセス制御装置。

【請求項 2】 ネットワークと、前記ネットワークに接続されたホストとのアクセスを制御するアクセス制御装置において、

アクセス制御ルールが格納されたアクセス制御テーブルと、

前記ネットワークから前記ホストへのアクセス要求があった場合に、要求されたアクセスを、前記アクセス制御テーブルから検索する検索手段と、

前記検索手段が前記アクセスを前記アクセス制御テーブルから見いだせなかった場合に、前記発信元にアクセス拒否を送信する拒否手段と、

前記検索手段が前記発信元を前記アクセス制御テーブルから見いだせた場合に、前記アクセス制御テーブルに格納されたアクセス制御ルールに基づき、アクセスを実行させるアクセス制御手段と、

バイオメトリクス認証結果を第 3 者に渡す認証サーバから、アクセス制御ルールの設定依頼が送信されてきた場合に、前記アクセス制御テーブルの内容を変更、追加又は削除するアクセス制御ルール管理手段と、

を含むことを特徴とするアクセス制御装置。

【請求項 3】 認証すべき人のバイオメトリックデータが予め格納されている認証テーブルと、

実行したい希望アクセス内容とバイオメトリックデータとを含む認証依頼を受信した場合に、前記バイオメトリックデータを前記認証テーブル中から検索する検索手段と、

前記検索手段が前記バイオメトリックデータを前記認証テーブル中から見いだせた場合に、前記認証依頼に含まれる希望アクセス内容を許可するようなアクセス制御ルールを設定するように外部のアクセス制御装置に依頼す

る依頼手段と、

を含むことを特徴とする認証装置。

【請求項 4】 ネットワーク上の所定のホストにアクセスしようとした際に、そのアクセスが拒否された場合に、所定の認証装置に認証依頼を送信する認証依頼手段、

を含み、

前記認証依頼には、自己を示す識別子と、自己が実行しようとする希望アクセス内容と、自己を示すデータであるバイオメトリックデータと、が含まれることを特徴とするネットワークアクセス装置。

【請求項 5】 第 1 ネットワークと、第 2 ネットワーク間のアクセスを制御するアクセス制御ルールが格納されたアクセス制御テーブルを備えたコンピュータを、前記第 1 ネットワークと、前記第 2 ネットワーク間のアクセスを制御するアクセス制御装置として動作させるためのプログラムにおいて、

前記コンピュータに、

前記第 1 ネットワークから第 2 ネットワークへのアクセス要求があった場合に、要求されたアクセスを、前記アクセス制御テーブルから検索する検索手順と、

前記検索手順において前記アクセスを前記アクセス制御テーブルから見いだせなかった場合に、前記発信元にアクセス拒否を送信する拒否手順と、

前記検索手順において前記発信元を前記アクセス制御テーブルから見いだせた場合に、前記アクセス制御テーブルに格納されたアクセス制御ルールに基づき、アクセスを実行させるアクセス制御手順と、

バイオメトリクス認証結果を第 3 者に渡す認証サーバから、アクセス制御ルールの設定依頼が送信されてきた場合に、前記アクセス制御テーブルの内容を変更、追加又は削除するアクセス制御ルール管理手順と、

を実行させることを特徴とするアクセス制御プログラム。

【請求項 6】 ネットワークと、前記ネットワークに接続されたホストとのアクセスを制御するアクセス制御ルールが格納されたアクセス制御テーブルを備えたコンピュータを、前記ネットワークと、前記ネットワークに接続された前記ホストとのアクセスを制御するアクセス制御装置として動作させるプログラムにおいて、

前記コンピュータに、

前記ネットワークから前記ホストへのアクセス要求があった場合に、要求されたアクセスを、前記アクセス制御テーブルから検索する検索手順と、

前記検索手順において前記アクセスを前記アクセス制御テーブルから見いだせなかった場合に、前記発信元にアクセス拒否を送信する拒否手順と、

前記検索手順において前記発信元を前記アクセス制御テーブルから見いだせた場合に、前記アクセス制御テーブルに格納されたアクセス制御ルールに基づき、アクセス

を実行させるアクセス制御手順と、
バイオメトリクス認証結果を第3者に渡す認証サーバから、アクセス制御ルールの設定依頼が送信されてきた場合に、前記アクセス制御テーブルの内容を変更、追加又は削除するアクセス制御ルール管理手順と、
を実行させることを特徴とするアクセス制御プログラム。

【請求項7】 認証すべき人のバイオメトリックデータが予め格納されている認証テーブルを備えたコンピュータを、認証装置として動作させるプログラムにおいて、
前記コンピュータに、
実行したい希望アクセス内容とバイオメトリックデータを含む認証依頼を受信した場合に、前記バイオメトリックデータを前記認証テーブル中から検索する検索手順と、
前記検索手順において前記バイオメトリックデータを前記認証テーブル中から見いだせた場合に、前記認証依頼に含まれる希望アクセス内容を許可するようなアクセス制御ルールを設定するように外部のアクセス制御装置に依頼する依頼手順と、
を実行させることを特徴とする認証プログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ネットワーク上のアクセスコントロールを動的に変更しうる装置及びその装置を構成するためのプログラムに関する。

【0002】

【従来の技術】ネットワーク上の各ホスト（端末やサーバ、クライアント、ルータ等のネットワーク上の1個の主体）を識別するために、たとえばインターネットではIPアドレスと呼ばれるアドレスが用いられている。ネットワーク上の各ホストは、このIPアドレスを用いて通信の相手先を指定している。

【0003】しかし、ネットワーク上の各ホストが自由に他のホストにアクセスできるわけではない。一般にセキュリティ上の問題や、管理上の都合により、あるホストに対するアクセスが制限されたり、あるホストからの発信が制限される場合は多い。

【0004】このような制御をするために、ファイアウォールやルータ、ブリッジと呼ばれる装置が使用されており、また、各ホスト毎にアクセスを制御するためにパーソナルファイアウォールと呼ばれるプログラムも知られている。

【0005】

【発明が解決しようとする課題】このように、ファイアウォールやルータ、ブリッジを用いて各種のアクセス制御が実行されていたが、この制御ルールはIPアドレスを用いて記述される場合が多い。たとえば、IPアドレス100.100.100.0からIPアドレス100.100.200.XXXに対するアクセスは認めら

れない（XXXは任意の数）等のようなものである。

【0006】しかし、近年、ダイヤルアップによるインターネットアクセスに代表されるように、同じIPアドレスが常に同じ人（や装置）に利用されるとは限らない状況が一般的になっている。このようなIPアドレスがダイナミックに割り当てられる状況の下では、IPアドレスを用いた固定的なアクセス制御ルールだけでは実際の利用形態に対応できない場合も想定される。

【0007】たとえば、あるIPアドレスは今日は課長が使用しているが、明日は部長が使用するかもしれない。この場合、課長と部長のアクセス権限が異なることも考えられるので、今日と明日で同じ固定的なアクセス制御ルールでは、実態に対処することは困難である。

【0008】本発明は、このような課題に鑑みなされたものであり、アクセス制御ルールを動的に変更しうる装置やプログラムを提供することである。

【0009】

【課題を解決するための手段】上記課題を解決するために、本発明は、第1ネットワークと、第2ネットワーク間のアクセスを制御するアクセス制御装置において、アクセス制御ルールが格納されたアクセス制御テーブルと、前記第1ネットワークから第2ネットワークへのアクセス要求があった場合に、要求されたアクセスを、前記アクセス制御テーブルから検索する検索手段と、前記検索手段が前記アクセスを前記アクセス制御テーブルから見いだせなかった場合に、前記発信元にアクセス拒否を送信する拒否手段と、前記検索手段が前記発信元を前記アクセス制御テーブルから見いだせた場合に、前記アクセス制御テーブルに格納されたアクセス制御ルールに基づき、アクセスを実行させるアクセス制御手段と、バイオメトリクス認証結果を第3者に渡す認証サーバから、アクセス制御ルールの設定依頼が送信されてきた場合に、前記アクセス制御テーブルの内容を変更、追加又は削除するアクセス制御ルール管理手段と、を含むことを特徴とするアクセス制御装置である。

【0010】このような構成によって、アクセス制御ルールを動的に変更等することができ。

【0011】また、本発明は、ネットワークと、前記ネットワークに接続されたホストとのアクセスを制御するアクセス制御装置において、アクセス制御ルールが格納されたアクセス制御テーブルと、前記ネットワークから前記ホストへのアクセス要求があった場合に、要求されたアクセスを、前記アクセス制御テーブルから検索する検索手段と、前記検索手段が前記アクセスを前記アクセス制御テーブルから見いだせなかった場合に、前記発信元にアクセス拒否を送信する拒否手段と、前記検索手段が前記発信元を前記アクセス制御テーブルから見いだせた場合に、前記アクセス制御テーブルに格納されたアクセス制御ルールに基づき、アクセスを実行させるアクセス制御手段と、バイオメトリクス認証結果を第3者に渡

す認証サーバから、アクセス制御ルールの設定依頼が送信されてきた場合に、前記アクセス制御テーブルの内容を変更、追加又は削除するアクセス制御ルール管理手段と、を含むことを特徴とするアクセス制御装置である。

【0012】このような構成によって、パーソナルファイアーウォールにおいてもアクセス制御ルールを動的に変更等することができる。

【0013】また、本発明は、認証すべき人のバイOMETリックデータが予め格納されている認証テーブルと、実行したい希望アクセス内容とバイOMETリックデータとを含む認証依頼を受信した場合に、前記バイOMETリックデータを前記認証テーブル中から検索する検索手段と、前記検索手段が前記バイOMETリックデータを前記認証テーブル中から見いだせた場合に、前記認証依頼に含まれる希望アクセス内容を許可するようなアクセス制御ルールを設定するように外部のアクセス制御装置に依頼する依頼手段と、を含むことを特徴とする認証装置である。

【0014】このような構成によって、バイOMETリックデータによる認証結果を外部に送信することができる。

【0015】また、本発明は、ネットワーク上の所定のホストにアクセスしようとした際に、そのアクセスが拒否された場合に、所定の認証装置に認証依頼を送信する認証依頼手段、を含み、前記認証依頼には、自己を示す識別子と、自己が実行しようとする希望アクセス内容と、自己を示すデータであるバイOMETリックデータと、が含まれることを特徴とするネットワークアクセス装置である。

【0016】このような構成によって、アクセスが拒否された場合に自動的に認証依頼を発することができる。

【0017】以下に述べる手段は、上記装置に関する手段を、プログラムとして表現したものであり、その本質的な特徴・作用は、上記装置に関する手段と同様である。

【0018】すなわち、本発明は、第1ネットワークと、第2ネットワーク間のアクセスを制御するアクセス制御ルールが格納されたアクセス制御テーブルを備えたコンピュータを、前記第1ネットワークと、前記第2ネットワーク間のアクセスを制御するアクセス制御装置として動作させるためのプログラムにおいて、前記コンピュータに、前記第1ネットワークから第2ネットワークへのアクセス要求があった場合に、要求されたアクセスを、前記アクセス制御テーブルから検索する検索手段と、前記検索手段において前記アクセスを前記アクセス制御テーブルから見いだせなかった場合に、前記発信元にアクセス拒否を送信する拒否手段と、前記検索手段において前記発信元を前記アクセス制御テーブルから見いだせた場合に、前記アクセス制御テーブルに格納されたアクセス制御ルールに基づき、アクセスを実行させる

アクセス制御手順と、バイOMETRICS認証結果を第3者に渡す認証サーバから、アクセス制御ルールの設定依頼が送信されてきた場合に、前記アクセス制御テーブルの内容を変更、追加又は削除するアクセス制御ルール管理手段と、を実行させることを特徴とするアクセス制御プログラムである。

【0019】また、本発明は、ネットワークと、前記ネットワークに接続されたホストとのアクセスを制御するアクセス制御ルールが格納されたアクセス制御テーブルを備えたコンピュータを、前記ネットワークと、前記ネットワークに接続された前記ホストとのアクセスを制御するアクセス制御装置として動作させるプログラムにおいて、前記コンピュータに、前記ネットワークから前記ホストへのアクセス要求があった場合に、要求されたアクセスを、前記アクセス制御テーブルから検索する検索手段と、前記検索手段において前記アクセスを前記アクセス制御テーブルから見いだせなかった場合に、前記発信元にアクセス拒否を送信する拒否手段と、前記検索手段において前記発信元を前記アクセス制御テーブルから見いだせた場合に、前記アクセス制御テーブルに格納されたアクセス制御ルールに基づき、アクセスを実行させるアクセス制御手順と、バイOMETRICS認証結果を第3者に渡す認証サーバから、アクセス制御ルールの設定依頼が送信されてきた場合に、前記アクセス制御テーブルの内容を変更、追加又は削除するアクセス制御ルール管理手段と、を実行させることを特徴とするアクセス制御プログラムである。

【0020】また、本発明は、認証すべき人のバイOMETリックデータが予め格納されている認証テーブルを備えたコンピュータを、認証装置として動作させるプログラムにおいて、前記コンピュータに、実行したい希望アクセス内容とバイOMETリックデータとを含む認証依頼を受信した場合に、前記バイOMETリックデータを前記認証テーブル中から検索する検索手段と、前記検索手段において前記バイOMETリックデータを前記認証テーブル中から見いだせた場合に、前記認証依頼に含まれる希望アクセス内容を許可するようなアクセス制御ルールを設定するように外部のアクセス制御装置に依頼する依頼手段と、を実行させることを特徴とする認証プログラムである。

【0021】

【発明の実施の形態】以下、本発明の好適な実施の形態を図面に基づいて説明する。

【0022】実施の形態1（ファイアーウォール）

図1には、本発明の好適な実施の形態であるファイアーウォール10を含むネットワーク構成図が示されている。

【0023】この図に示すように、ファイアーウォール10は、インターネット12と、ローカルネットワーク14とに接続している。このローカルネットワーク14

には、WEBサーバ16と認証サーバ18とが接続している。また、インターネット12には、外部端末20が接続している。

【0024】このファイアウォール10は、請求の範囲の「アクセス制御装置」の一例に相当する。また、認証サーバ18は、請求の範囲の「認証装置」の一例に相当する。また、外部端末20は、請求の範囲の「ネットワークアクセス装置」の一例に相当する。

【0025】インターネット12側の外部端末20からは、ローカルネットワーク14内のアドレスは直接見えずに、ローカルネットワーク14に対して代表となるIPアドレスが1個割り当てられている。この代表となるIPアドレスは直接的には、ファイアウォール10のIPアドレスである。

【0026】外部端末20からローカルネットワーク14のWEBサーバ16にアクセスする場合には、この代表的なIPアドレス（ファイアウォール10のIPアドレス）にアクセスし、利用するポート番号としてたとえば80を指定するのである。このポート番号によって、ファイアウォール10は、外部端末20がWEBサービスを利用したいということを知り、外部端末20からのアクセスをWEBサーバ16に送り出すのである。

【0027】なお、ここでは、WEBサービスのポート番号として80を利用したが、その他のポート番号でも良い。このようにポート番号で指定することによって、ローカルネットワーク14内の各ホストを識別している。

【0028】ファイアウォール10の構成
ファイアウォール10の構成ブロック図が図2に示されている。この図に示すように、ファイアウォール10は、インターネット12の外部端末20からのアクセス要求を受け、その要求されたアクセスをアクセス制御テーブル26中のアクセス制御ルールから検索する検索手段22と、検索した結果、見いだせなかった場合にそのアクセスを拒否する拒否手段24とが備えられている。

【0029】また、ファイアウォール10は、検索手段22が、要求されたアクセスを、アクセス制御テーブル26中から見いだした場合に、その要求されたアクセスを実行するアクセス制御手段28と、アクセス制御テーブル26の内容であるアクセス制御ルールを管理するアクセス制御ルール管理手段30とを備えている。

【0030】本実施の形態において特徴的なことはアクセス制御テーブル26中のアクセス制御ルールが動的に追加、変更、削除される点である。この点に関しては、後に詳述する。

【0031】アクセス制御ルールは、一般に、認められるアクセスを記述したものであり、アクセス制御テーブル26は複数のアクセス制御ルールを集めた表である。

【0032】アクセス制御テーブル26の内容を表す説明図が図3に示されている。この図に示すように、アクセス制御テーブル26の各エントリ（すなわち、認められるアクセスを記述したアクセス制御ルール）は、発信元の情報と、発信先の情報と、から構成されている。発信元の情報とは、発信元のIPアドレス及びポート番号であり、発信先の情報とは、発信先のIPアドレス及びポート番号である。なお、この表中Xはいわゆるワイルドカードであり、すべての番号を表す記号である。また、表中では、ある特定の数字が記述される例を示しているが、一定の範囲、たとえば100.100.100.100～100.100.100.300のような範囲で示しても良い。ファイアウォール10は、この図3の表に示されていない組み合わせのアクセスを拒否する。

【0033】なお、ファイアウォール10中の検索手段22、アクセス拒否手段24、アクセス制御手段28、アクセス制御ルール管理手段30は、プログラムとそのプログラムを実行するプロセッサから構成されることが好ましい。また、アクセス制御テーブル26はハードディスク等の上に構築されることが好ましい。このプロセッサとは、請求の範囲の「コンピュータ」の一例に相当する。

【0034】認証サーバ18の構成
認証サーバ18の構成ブロック図が図4に示されている。本実施の形態における認証サーバ18は、バイオメトリックデータによって個人認証を行うサーバである。バイオメトリックデータとしては署名データを利用しているが、他のバイオメトリックデータ、たとえば指紋データや、網膜パターン等でもかまわない。

【0035】図4に示すように、認証サーバ18は、署名データが予め登録されている認証テーブル40と、外部からの依頼によって認証テーブル40を検索する検索手段42とを備えている。また、認証サーバ18は、ファイアウォール10等のアクセス制御装置に、アクセス制御ルールの調整（追加、変更、削除など）を依頼する依頼手段44を備えている。このような構成によって、署名データによって認証された利用者が希望するアクセスを許可するようなアクセス制御ルールがファイアウォール10に設定される。

【0036】なお、検索手段42、依頼手段44は、プログラムとこのプログラムを実行するプロセッサとから構成することが望ましい。また、認証テーブル40はハードディスク等の上に構築することが望ましい。

【0037】外部端末20の構成
外部端末20の構成ブロック図が図5に示されている。この図に示すように、外部端末20は、WEBサーバ16に接続し、WEBページを閲覧するためのWEB閲覧手段46と、アクセスが拒否された場合に外部の認証サーバ18に認証を依頼する認証依頼手段48と、を備え

ている。

【0038】WEB閲覧手段46は、いわゆるブラウザと呼ばれるプログラム（及びそれを実行するプロセッサ）で構成することが望ましい。このプログラムを用いてWEBサーバ16が提供するWEBページをディスプレイ49に表示する。認証依頼手段48も、プログラムとそれを実行するプロセッサから構成されることが望ましい。したがって典型的には、この外部端末20はブラウザなどのプログラムがインストールされたコンピュータで実現される。もちろん、PDA（Personal Digital Assistant）や携帯電話等、インターネット12に接続しうる装置であればそのような装置でもかまわない。

【0039】動作

以下、本実施の形態におけるアクセスの処理の流れをフローチャートに基づき説明する。図6、図7には、この動作を表すフローチャートが示されている。

【0040】まず、ステップS6-1においては、外部端末20がWEBサーバ16に対してアクセスを行おうとする。このアクセスは、WEB閲覧手段46によって実行される。

【0041】ステップS6-2においては、このアクセス要求は、ファイアウォール10に受信され、ファイアウォール10がこのアクセスがアクセス制御テーブルに記載されているか検索が行われる。この検索は、検索手段22によって実行される。検索は、発信元と発信先のIPアドレス及びポート番号が、アクセス制御テーブル26中に記載されているか否かを検査することによって実行される。記載されていれば、それはアクセスが許可されていることを意味し、ステップS6-3に処理が移行する。一方、記載されていない場合は、ステップS6-4に処理が移行する。

【0042】ステップS6-3においては、アクセスが許可されているので、そのままアクセスを認める。すなわち、WEBサーバ16（ポート番号：80）に外部端末20からの送信データを転送するのである。

【0043】ステップS6-4においては、許可されていない者からのアクセスであると判断し、アクセス拒否を外部端末20に送信する。この拒否動作は、アクセス拒否手段24によって実行される。

【0044】ステップS6-5においては、アクセスを拒否された外部端末20が許可を得るために認証サーバ18に認証依頼を送信する。認証依頼手段48がこの動作を実行する。本実施の形態において特徴的なことは、この認証依頼中に、外部端末20の利用者のIDと利用者の署名データとが含まれていることである。さらに、認証依頼中には、実行したいアクセスの内容を含むことができる。

【0045】なお、このIDは、請求の範囲の「識別子」の一例である。また、署名データは請求の範囲中の「バイオメトリックデータ」の一例である。また、実行

したいアクセスの内容は、請求の範囲中の「希望アクセス内容」に該当する。この実行したいアクセスの内容は、自己のIPアドレスやポート番号、及びアクセスの相手先のIPアドレスやポート番号が含まれる。また、実行したいアクセスの内容中に、アクセスを開始したい時刻や、終了したい時刻を含めても良い。

【0046】実行したいアクセスの内容（希望アクセス内容）は、サーバ側のポリシーとの組み合わせで、実際のアクセスルールがファイアウォール10に適用される。なお、サーバ側とは、認証サーバ18（認証装置）、ファイアウォール10（アクセス制御装置のいずれかを言う。しかし、認証サーバ18がポリシーを持つのが一般的であろう。たとえば、外部端末20（クライアント）から社員Aのアカウントで役員BのPCに対するアクセス許可を希望した場合でも、認証装置側に役員BのPCには役員自身が認証を行わないとアクセスを許可しないようにポリシー設定されている場合その希望は許可されない。極端に言えば、外部端末20（クライアント）側から希望が出されなくても認証サーバ18（認証装置）側に設定されたポリシーにしたがってファイアウォール10（アクセス制御装置）にルールを適用することも好ましい。

【0047】この認証サーバ18のポート番号はたとえば9999に設定されており、誰でもアクセスが許可されているポートとして設定されている。

【0048】ステップS6-6においては、認証サーバ18が上記認証依頼を受信し、認証動作を実行する。具体的には、認証サーバ18の検索手段42が、認証依頼中の署名データを認証テーブル40から検索する。その後図7のステップS7-1に処理が移行する。

【0049】ステップS7-1において、認証依頼中の署名データと同一人による署名データであると認められるほど近似した署名データが認証テーブル40中に見いだされた場合には、ステップS7-2に処理が移行し、アクセス制御ルールの調整が行われる。一方、同一人による署名データと認められる署名データが認証テーブル40中になかった場合には、ステップS7-4に処理が移行する。

【0050】ステップS7-2においては、認証依頼中に含まれていた「実行したいアクセス内容」を許可するアクセス制御ルールを、ファイアウォール10に設定するように依頼が行われる。この依頼は、依頼手段44が実行する。

【0051】ステップS7-3においては、上記依頼に基づき、ファイアウォール10がアクセス制御ルールをアクセス制御テーブル26に登録する。

【0052】このように、本実施の形態によれば、動的にアクセス制御テーブル26中のアクセス制御ルールが調整される。すなわち、一つのIPアドレスを複数人が共有している場合でも、現在の使用者に対応したアクセ

ス制御ルールが設定できるので、円滑なネットワークの利用が可能である。

【0053】アクセス制御ルールが変更された後は、外部端末20からWEBサーバ16に対するアクセスが許可される。具体的には、図6におけるステップS6-1、S6-2、S6-3の流れの処理が実行される。

【0054】ステップS7-4においては、認証拒否（失敗）が外部端末20に送信される。

【0055】このように、本実施の形態によれば、バイオメトリックデータ（署名データ）により、本人を認証し、これに基づいてアクセス制御ルールを動的に変更する仕組みが実現されている。

【0056】アクセス制御ルールの調整

上述したように動的に調整（変更、追加、削除）されたアクセス制御ルールは、所定期間経過した場合、又は、アクセスが所定期間以上なかった場合に、元に戻すことが望ましい。これによって、一時的なアクセス制御ルールの調整に対応することができるのである。

【0057】実施の形態2A（ルータ装置）

実施の形態1では、請求の範囲の「アクセス制御装置」の例としてファイアーウォール10を説明したが、ファイアーウォールの代わりにルータ装置を利用することも好ましい。この場合のアクセス制御ルールには、ルーティング（Routing）・ルールを含むことができる。また、ルータは、2つのネットワーク間に設けられるだけでなく、複数のネットワークに接続しうるものであるので、このルーティング・ルールも一般的には複数のネットワーク間のルーティングに関するルールである。

【0058】このようにルータ装置によれば、IPアドレスの利用者のバイオメトリックデータによって、ルーティング・ルールを含めたアクセス制御ルールを動的に変更することができる。

【0059】なお、請求の範囲における「アクセス制御ルール」はアクセスに関するルールであればどのようなルールでもかまわない。たとえば、グローバルIPアドレスとローカルアドレスとの変換を行うルールでも良い。

【0060】実施の形態2B（ブリッジ）

また、ファイアーウォール10の代わりに、ブリッジと呼ばれる装置を利用することも好ましい。このブリッジはネットワークを接続する装置として知られているが、この接続状況を表すルールがアクセス制御ルールとなる。このブリッジも請求の範囲の「アクセス制御装置」の一例に相当する。

【0061】この接続状況を表すルールを利用者のバイオメトリックデータによって動的に変化させることが可能である。

【0062】実施の形態3（認証サーバの一体化）

なお、実施の形態1では、ファイアーウォール10と認証サーバ18は別体に構成したが、一体に構成すること

も好ましい。この場合、ファイアーウォール10中に認証サーバ18が組み込まれる形態となる。

【0063】このような形態を実現するためには、ファイアーウォール10中に、認証サーバ18の動作を実行するプログラムを組み込み、またハードディスク等の上に認証テーブル40を構築するのが好ましい。

【0064】この一体に構成した場合は、請求の範囲の「ネットワーク装置」の一例に相当し、その中のファイアーウォール10に該当する機能は請求の範囲の「アクセス制御ユニット」に、認証サーバ18に該当する機能は請求の範囲の「認証ユニット」に、それぞれ相当する。

【0065】実施の形態4（ホストベースファイアーウォール）

上記の例では、ネットワーク間のファイアーウォール10について説明したが、1個のローカル端末50とインターネット12との間に設けられるファイアーウォールにアクセス制御ルールの動的な変更の動作を持たせることも好ましい。このような1個のローカル端末50に関してアクセスの制御を行ってその外部端末を保護する装置を、本特許明細書では、ホストベースファイアーウォール52と呼ぶ。

【0066】このようなホストベースファイアーウォール52を中心としたネットワーク構成図が図8に示されている。この図に示すように、ローカル端末50は、ホストベースファイアーウォール52を介してインターネット12に接続する構成である。このローカル端末50上では、HTTPプログラムが起動しており、ローカル端末50は、WEBサーバ16の動作を実行している。そして、外部端末20から、このホストベースファイアーウォール52を介してWEBサーバ16（ローカル端末50）に接続しようとする。

【0067】ホストベースファイアーウォール52の構成は、図2に示したファイアーウォール10とほぼ同様である。異なる点は、ネットワーク間のアクセス制御ではなく、ネットワークとローカル端末との間のアクセス制御を行う点と、アクセス制御ルール管理手段に対する依頼が、ローカルネットワークではなくインターネット12側から来る点である。その他の点は図2の構成と同様である。

【0068】また、本実施の形態における動作も、上記図6及び図7に示した動作と同様である。

【0069】本実施の形態によれば、ローカル端末50を保護するホストベースファイアーウォール52のアクセス制御ルールをバイオメトリックデータの一つである署名データによる認証を介して動的に変更することができる。したがって、同じIPアドレスを複数人が共同で使用する場合等においても、ローカル端末50を効果的に保護することができる。

【0070】なお、このホストベースファイアーウォー

ル 5 2 も、請求の範囲の「アクセス制御装置」の一例に相当する。

【0071】実施の形態 5（端末との一体化）

実施の形態 4 では形式的には、ハードウェアでホストベースファイアウォール 5 2 を構成した。しかし、このホストベースファイアウォール 5 2 をローカル端末 5 0 上で稼働するプログラムで実現しても良い。

【0072】実施の形態 6 A（認証サーバとの一体化）

なお、実施の形態 4 では、ホストベースファイアウォール 5 2 と認証サーバ 1 6 は別体に構成したが、一体に 10 構成することも好ましい。この場合、ファイアウォール 1 0 中に認証サーバ 1 8 が組み込まれる形態となる。

【0073】このような形態を実現するためには、ホストベースファイアウォール 5 2 中に、認証サーバ 1 6 の動作を実行するプログラムを組み込み、またハードディスク等の上に認証テーブル 4 0 を構築するのが好ましい。

【0074】このような構成は、請求の範囲の「ネットワーク装置」の一例に相当する。

【0075】実施の形態 6 B（端末及び認証サーバとの 20 一体化）

なお、実施の形態 6 A のようにホストベースファイアウォール 5 2 と認証サーバ 1 8 とを一体に構成する場合も、これらをローカル端末 5 0 上で稼働するプログラムで実現しても良い。

【0076】すなわち、ローカル端末 5 0 中に、ホストベースファイアウォール 5 2 の動作を実行するプログラムを組み込むと共に、ハードディスク等の上にアクセス制御テーブル 2 6 を構築するのである。さらに、ローカル端末 5 0 中に、認証サーバ 1 8 の動作を実行するプ 30 ログラムを組み込み、またハードディスク等の上に認証テーブル 4 0 を構築するのである。このような構成によって、ローカル端末 5 0 上で稼働するプログラムを用いて、ホストベースファイアウォール 5 2 及び認証サーバ 1 8 を実現することができる。

【0077】

【発明の効果】以上述べたように、本発明によれば、バ

イオメトリックデータによる認証に基づきアクセス制御ルールを動的に変更等することができるので、アドレスを利用する者の変更等に迅速に対処することができる。

【図面の簡単な説明】

【図 1】本発明の好適な実施の形態 1 のファイアウォールを含むネットワーク構成図である。

【図 2】ファイアウォールの構成ブロック図である。

【図 3】アクセス制御テーブルの内容を表す説明図である。

【図 4】認証サーバの構成ブロック図である。

【図 5】外部端末の構成ブロック図である。

【図 6】本実施の形態におけるアクセスの処理の流れを表すフローチャートである。

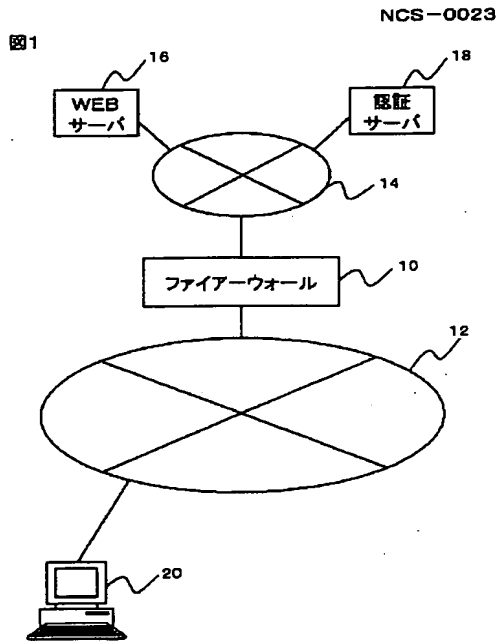
【図 7】本実施の形態におけるアクセスの処理の流れを表すフローチャートである。

【図 8】ホストベースファイアウォールを中心としたネットワーク構成図である。

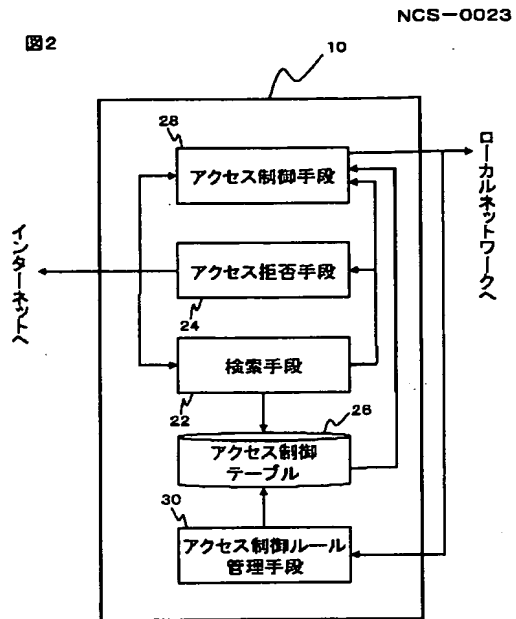
【符号の説明】

- 10 ファイアウォール
- 12 インターネット
- 14 ローカルネットワーク
- 16 WEBサーバ
- 18 認証サーバ
- 20 外部端末
- 22 検索手段
- 24 アクセス拒否手段
- 26 アクセス制御テーブル
- 28 アクセス制御手段
- 30 アクセス制御ルール管理手段
- 40 認証テーブル
- 42 検索手段
- 44 依頼手段
- 46 WEB閲覧手段
- 48 認証依頼手段
- 49 ディスプレイ
- 50 ローカル端末
- 52 ホストベースファイアウォール

【図1】



【図2】



【図3】

図3

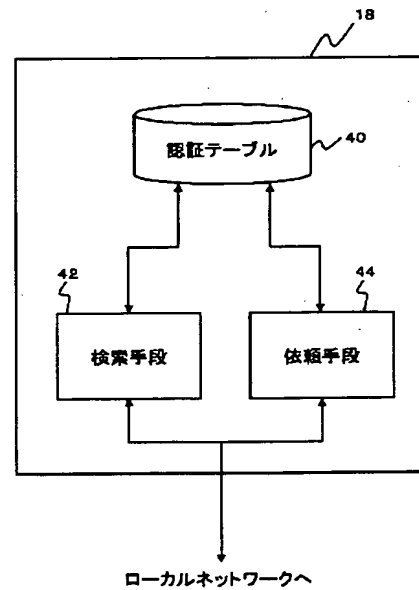
NCS-0023

発信元		発信先	
IPアドレス	ポート番号	IPアドレス	ポート番号
100.100.100.0	5	100.100.200.XXX	XX
100.100.XXX.XXX	XX	100.100.200.0	80
XXX.XXX.XXX.XXX	XX	100.100.200.0	9999
⋮	⋮	⋮	⋮

【図4】

図4

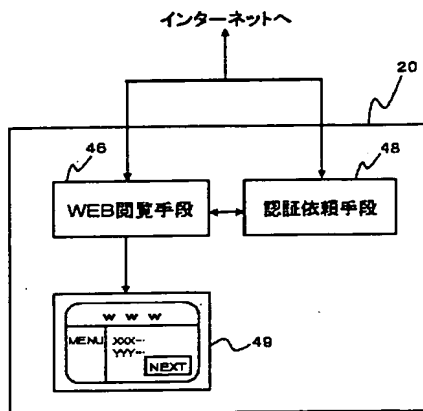
NCS-0023



【図 5】

NCS-0023

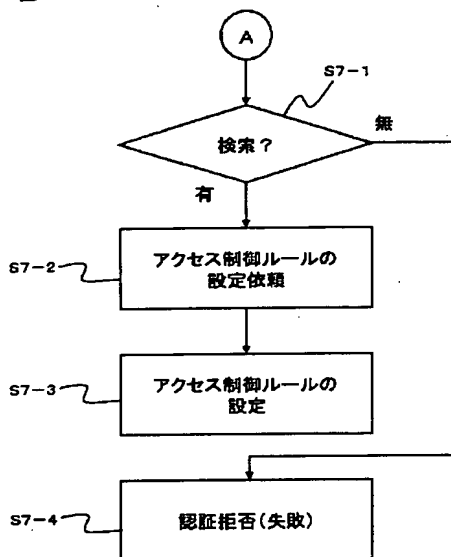
図5



【図 7】

NCS-0023

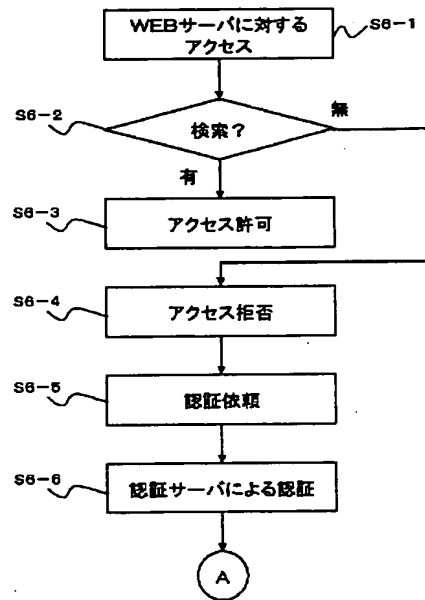
図7



【図 6】

NCS-0023

図6



【図 8】

NCS-0023

図8

